



Avaya Solution & Interoperability Test Lab

Application Notes for First In Line™ by Swampfox Technologies, Inc with Avaya Aura® Application Enablement Services and Avaya Aura® Experience Portal – Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate First In Line™ by Swampfox Technologies, Inc with Avaya Aura® Application Enablement Services and Avaya Aura® Experience Portal.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration steps required to integrate First In Line™ (FIL) by Swampfox Technologies, Inc with Avaya Aura® Application Enablement Services (AES) and Avaya Aura® Experience Portal (Experience Portal). FIL offers contact center callers the ability to request a callback if agents are unavailable. FIL offers the following features to contact center callers:

- **Automated Callback:** Monitors overall customer experience through calculation of customer specific Expected Wait Time (EWT) and offers customer options to opt-in for immediate or scheduled callback.
- **Immediate Callback:** Manages position within queue for requested agent skills and proactively calls customer first and then connects to proper agent, virtually holding their place in line.
- **Scheduled Callback:** Offers the ability for a customer to choose from a variety of times in the future to schedule a callback for the requested skill-set required to resolve their request.

FIL integrates with Experience Portal via VoiceXML application to offer callback requests to callers. FIL uses the outcall web service provided by Experience Portal to place calls to those callers who requested callbacks. FIL integrates with AES via TSAPI interface. FIL uses the Query Agent State Service provided by TSAPI to obtain agent states and calculate EWT.

The incoming contact center caller call flow follows:

- Customer calls the contact center and gets routed to Experience Portal via vector programming.
- Once the call is answered by the FIL application configured on Experience Portal, depending on EWT algorithm on FIL, call is either routed back to an agent queue on Communication Manager or offered a call back.
- If call back is offered, FIL detects the caller's phone number and offers a call back option.
- If customer decides to decline the callback option, call is routed back in queue on Communication Manager.
- FIL places the call back request to the caller via Experience Portal.
- Once the caller answers, call is transferred to agent queue (with high priority) on Communication Manager.

2. General Test Approach and Test Results

This section describes the interoperability compliance testing used to verify the FIL with AES and Experience Portal.

The interoperability compliance test included feature and serviceability testing. The feature testing focused on routing calls to Experience Portal and running the FIL application to allow the caller the option to request a call back. All of the call back request options available in the FIL Inbound application were tested. In addition, the FIL Outbound application was also verified. The Outbound module initiated the call back to the agent and caller and established a two-way talk path. Conditions where the call back could not be established were also verified. In these cases, the call was either rescheduled or marked as failed, if the number of retries were exceeded. Finally, the registered call back requests and call back status were verified in FIL reports.

The serviceability testing focused on verifying the ability of FIL server, and AES and Experience Portal to recover from adverse conditions, such as power failures and disconnecting network.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

2.1. Interoperability Compliance Testing

Interoperability compliance testing included feature and serviceability testing. The feature testing focused on the following functionality:

- Routing incoming calls to Experience Portal via SIP trunk.
- Experience Portal successfully running FIL application.
- The ability of the caller to continue waiting in queue for an agent.
- The ability of the caller to make a call back request. Various offered call back options were tested, such as immediate or scheduled.
- FIL servicing call back requests via Experience Portal.
- The ability to reschedule a call back if the call to the agent or caller is not completed within a specified timeout value.

The serviceability testing focused on verifying the ability of FIL to recover from adverse conditions, such as power and network failures.

2.2. Test Results

All executed test cases passed.

2.3. Support

For technical support on FIL, contact Swampfox Technologies, Inc via phone, email, or internet.

- **Phone:** +1 803 451 4542
- **Email:** phackett@swampfoxinc.com
- **Web:** support.swampfoxinc.com

3. Reference Configuration

Error! Reference source not found. **Figure 1** below depicts the lab configuration used for testing. In this configuration, Experience Portal interfaces with Communication Manager via SIP trunk. The FIL server hosted the FIL application. The FIL server also connected to AES via TSAPI.

Note that SIP connectivity between Communication Manager, Session Manager and Experience Portal is standard in nature, and as such, it is not included in this document. Please refer to documentation in **Section 11**.

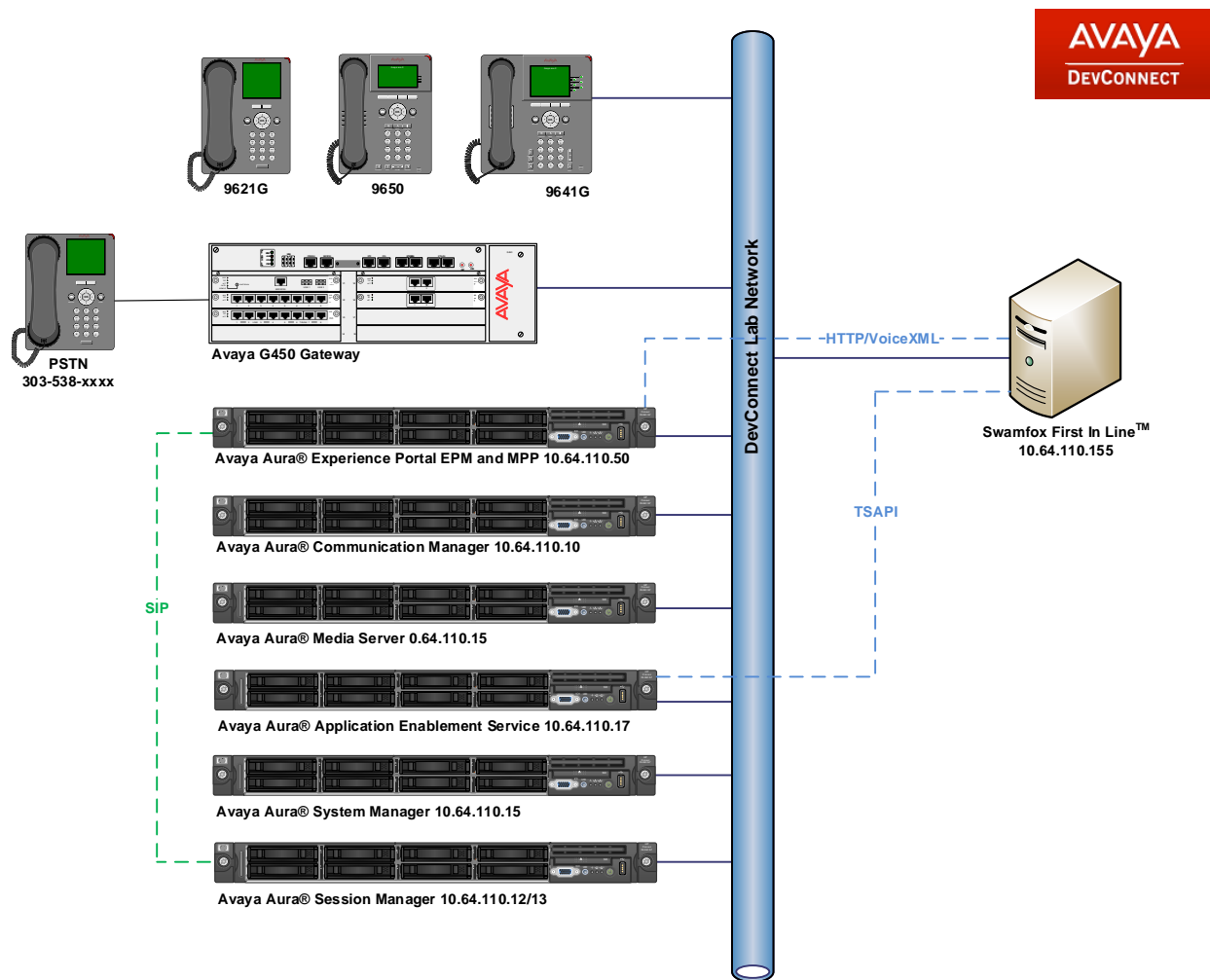


Figure 1: Test Configuration Diagram

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on Virtualized Environment	7.1.3 R017x.01.0.532.0 Build 24515
Avaya Aura® Application Enablement Services running on Virtualized Environment	7.1.3.0.1.7-0
Avaya Aura® Media Server running on Virtualized Environment	7.8
Avaya Aura® Experience Portal running on Virtualized Environment	7.2.1.0.0605
Avaya G450 Media Gateway	38.19.0
Avaya 9641GS H.323 IP Deskphone	6.6.6
Avaya 9621G SIP IP Deskphone	7.1.29
Swampfox Technologies, Inc First In Line™ running on a Virtualized Environment	2.0.3 CentOS 6.10 Final
Avaya TSAPI Client and SDK	Avaya JTAPI 7.1.0.8

5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager via the System Access Terminal (SAT). The procedures include the following areas:

- Administer System Parameters Features
- Administer Hunt Groups for Agents
- Administer Agent IDs for Agents
- Administer Call Vectoring
- Administer AES Connectivity
- Administer SIP Trunks
- Administer AAR Table
- Administer AES Connectivity

5.1. Administer System Parameters Features

Configure **System Parameter Features** used during compliance test. On **Page 5**, enable **Create Universal Call ID** and provide a unique **UCID Network Node**.

change system-parameters features	Page 5 of 19
19	
FEATURE-RELATED SYSTEM PARAMETERS	
SYSTEM PRINTER PARAMETERS	
Endpoint:	Lines Per Page: 60
SYSTEM-WIDE PARAMETERS	
Switch Name:	
Emergency Extension Forwarding (min): 10	
Enable Inter-Gateway Alternate Routing? n	
Enable Dial Plan Transparency in Survivable Mode? n	
COR to Use for DPT: station	
EC500 Routing in Survivable Mode: dpt-then-ec500	
MALICIOUS CALL TRACE PARAMETERS	
Apply MCT Warning Tone? n MCT Voice Recorder Trunk Group:	
Delay Sending RElease (seconds): 0	
SEND ALL CALLS OPTIONS	
Send All Calls Applies to: station Auto Inspect on Send All Calls? n	
Preserve previous AUX Work button states after deactivation? n	
UNIVERSAL CALL ID	
Create Universal Call ID (UCID)? y UCID Network Node ID: 1	

On **Page 13**, enable **Copy ASAI UI During Conference/Transfer** and **Send UCID to ASAI**.

change system-parameters features	Page 13 of 19
FEATURE-RELATED SYSTEM PARAMETERS	
CALL CENTER MISCELLANEOUS	
Callr-info Display Timer (sec): 10	
Clear Callr-info: next-call	
Allow Ringer-off with Auto-Answer? n	
Reporting for PC Non-Predictive Calls? n	
Agent/Caller Disconnect Tones? n	
Interruptible Aux Notification Timer (sec): 3	
Zip Tone Burst for Callmaster Endpoints: double	
ASAI	
Copy ASAI UI During Conference/Transfer? y	
Call Classification After Answer Supervision? n	
Send UCID to ASAI? y	
For ASAI Send DTMF Tone to Call Originator? y	
Send Connect Event to ASAI For Announcement Answer? n	
Prefer H.323 Over SIP For Dual-Reg Station 3PCC Make Call? n	

5.2. Administer Hunt Groups

This section provides the Hunt Group configuration for the call center agents. Agents will log into Hunt Group 1 configured below. Provide a descriptive name and set the **Group Extension** field to a valid extension. Enable the **ACD**, **Queue**, and **Vector** options. This hunt group will be specified in the **Agent LoginIDs** configured in **Section 5.3**.

add hunt-group 21	Page 1 of 4
HUNT GROUP	
Group Number: 21	ACD? y
Group Name: FIL Skill 1	Queue? y
Group Extension: 22231	Vector? y
Group Type: ucd-mia	
TN: 1	
COR: 1	MM Early Answer? n
Security Code:	Local Agent Preference? n
ISDN/SIP Caller Display:	
Queue Limit: unlimited	
Calls Warning Threshold:	Port:
Time Warning Threshold:	Port:
SIP URI:	

On **Page 2** of the Hunt Group form, enable the **Skill** option.

add hunt-group 21	Page 2 of 4
HUNT GROUP	
Skill? y	Expected Call Handling Time (sec): 10
AAS? n	Service Level Target (% in sec): 80 in 20
Measured: both	
Supervisor Extension:	
Controlling Adjunct: none	
VuStats Objective:	
Multiple Call Handling: none	
Timed ACW Interval (sec): 20	After Xfer or Held Call Drops? n

5.3. Administer Agent IDs

This section provides the Agent Login IDs for the agents. Add an **Agent Login ID** for each agent in the call center as shown below. In this configuration, agent login IDs 55001, 55002 and 55003 were created for three call center agents.

add agent-loginID 55001		Page 1 of 2
AGENT LOGINID		
Login ID: 55001	AAS? n	
Name: Agent 1	AUDIX? n	
TN: 1	Check skill TNs to match agent TN? n	
COR: 1		
Coverage Path:	LWC Reception: spe	
Security Code:	LWC Log External Calls? n	
Attribute:	AUDIX Name for Messaging:	
LoginID for ISDN/SIP Display? n		
Password:		
Password (enter again):		
Auto Answer: station		
AUX Agent Remains in LOA Queue: system	MIA Across Skills: system	
AUX Agent Considered Idle (MIA): system	ACW Agent Considered Idle: system	
Work Mode on Login: system	Aux Work Reason Code Type: system	
Logout Reason Code Type: system		
Maximum time agent in ACW before logout (sec): system		
Forced Agent Logout Time: :		
WARNING: Agent must log in again before changes take effect		

On **Page 2** of the **Agent LoginID** form, set the skill number (**SN**) to hunt group 21, which is the hunt group (skill) that the agents will log into.

add agent-loginID 55001		Page 2 of 2
AGENT LOGINID		
Direct Agent Skill:		Service Objective? n
Call Handling Preference: skill-level		Local Call Preference? n
SN	RL SL	SN RL SL
1: 21	1	16:
2:		17:
3:		18:
4:		19:
5:		20:
6:		
7:		
8:		
9:		
10:		
11:		
12:		
13:		
14:		
15:		

5.4. Administer Call Vectoring

This section describes the procedures for configuring call vectoring for calls queued to agents and inbound calls to FIL. There were three VDNs created during the compliance test:

22221: Inbound calls and routing to Experience Portal and offered call backs

22222: Calls queue with medium priority

22223: Calls queue with high priority

These three VDNs were configured with vectors 21, 22 and 23, respectively.

VDN 22221 for inbound calls and routing to Experience Portal and offered call backs.

add vdn 22221	Page 1 of 3
VECTOR DIRECTORY NUMBER	
Extension: 22221	
Name*: FIL Inbound	
Destination: Vector Number	21
Attendant Vectoring? n	
Meet-me Conferencing? n	
Allow VDN Override? y	
COR: 1	
TN*: 1	
Measured: none	Report Adjunct Calls as
ACD*? n	
VDN of Origin Annc. Extension*:	
1st Skill*:	
2nd Skill*:	
3rd Skill*:	
SIP URI:	
* Follows VDN Override Rules	

On **Page 3**, configured variables. Set **V1** to the current VDN numbers. Set **V2** to the digits that will be used to route calls over to Experience Portal. Set **V3** to the VDN with medium priority.

add vdn 22221	Page 3 of 3
VECTOR DIRECTORY NUMBER	
VDN VARIABLES*	
Var	Description Assignment
V1	Queuing VDN 22221
V2	FIL Offer DNIS 851111
V3	No Callback 22222
V4	
V5	
VDN Time-Zone Offset*: + 00:00	
Daylight Saving Rule*: system	
Use VDN Time Zone For Holiday Vectoring*? n	
Apply Ringback for Auto Answer calls*? y	
* Follows VDN Override Rules	

VDN 22222 for call queue with medium priority. This VDN is used when FIL deems EWT hasn't crossed the threshold or caller decides to wait in queue, rejecting the callback.

add vdn 22222	Page 1 of 3
VECTOR DIRECTORY NUMBER	
Extension: 22222	
Name*: No Callback	
Destination: Vector Number	22
Attendant Vectoring? n	
Meet-me Conferencing? n	
Allow VDN Override? n	
COR: 1	
TN*: 1	
Measured: none	Report Adjunct Calls as
ACD*? n	
VDN of Origin Annc. Extension*:	
1st Skill*:	
2nd Skill*:	
3rd Skill*:	
SIP URI:	
* Follows VDN Override Rules	

VDN 22223 for call queue with high priority. This VDN is used after callback request is made to customer and the call is transfer to Communication Manager from Experience Portal.

add vdn 22223	Page 1 of 3
VECTOR DIRECTORY NUMBER	
Extension: 22223	
Name*: Callback	
Destination: Vector Number	23
Attendant Vectoring? n	
Meet-me Conferencing? n	
Allow VDN Override? n	
COR: 1	
TN*: 1	
Measured: none	Report Adjunct Calls as
ACD*? n	
VDN of Origin Annc. Extension*:	
1st Skill*:	
2nd Skill*:	
3rd Skill*:	
SIP URI:	
* Follows VDN Override Rules	

Following screen captures display the corresponding vectors for VDNs added above.

change vector 21	Page 1 of 6
CALL VECTOR	
Number: 21 Name: FIL Vector Inbound	
Multimedia? n	Attendant Vectoring? n Meet-me Conf? n Lock?
n	
Basic? y	EAS? y G3V4 Enhanced? y ANI/II-Digits? y ASAI Routing?
y	
Prompting? y	LAI? y G3V4 Adv Route? y CINFO? y BSR? y Holidays? y
Variables? y	3.0 Enhanced? y
01 wait-time	2 secs hearing ringback
02 set	J = V1 CATR none
03 route-to	number V2 with cov n if unconditionally
04 stop	

5.5. Administer SIP Trunks

For the SIP trunk between Communication Manager and Session Manager, on **Page 3**, set **UII Treatment** to **Shared** and **Send UCID** to **y**.

change trunk-group 2		Page 3 of 22
TRUNK FEATURES		
ACA Assignment? n	Measured: none	Maintenance Tests? y
Suppress # Outpulsing? n Numbering Format: private		
UII Treatment: shared		
Maximum Size of UII Contents: 128		
Replace Restricted Numbers? n		
Replace Unavailable Numbers? n		
Hold/Unhold Notifications? y		
Modify Tandem Calling Number: no		
Send UCID? y		
Show ANSWERED BY on Display? y		

5.6. Administer AAR table

During the compliance test, calls to Experience Portal were routed via SIP trunk to Session Manager. 51111 was used to route call to Session Manager. Configure the dial string as configured in **V2** for inbound VDN configured in **Section 5.4**. Route Pattern 2 corresponds to routing calls to Trunk Group 2, the trunk group between Session Manager and Communication Manager.

change aar analysis 51111						Page 1 of 2
AAR DIGIT ANALYSIS TABLE						
Location: all				Percent Full: 0		
Dialed	Total	Route	Call	Node	ANI	
String	Min Max	Pattern	Type	Num	Reqd	
51111	5 5	2	aar		n	

5.7. Administer AES Connectivity

Configuration for AES and CTI link used during compliance test is standard in nature and is outside the scope of this document. For more information, please refer to documentation in **Section 11**.

6. Configure Avaya Aura® Application Enablement Services

This section provides the procedures for configuring AES. Switch connection and TSAPI configuration for connectivity to Communication Manager were preconfigured and standard in nature; thus, not mentioned in this document.

FIL server connected to AES via TSAPI to monitor hunt group configured on Communication Manager. This includes:

- Administer User
- Obtain Tlink

Access the AES OAM web interface by using the URL “https://ip-address” in a web browser, where “ip-address” is the IP address of AES. Log on using appropriate credentials.



Application Enablement Services Management Console

[Help](#)


Please login here:

Username

Copyright © 2009-2016 Avaya Inc. All Rights Reserved.

6.1. Administer User

Once logged on, navigate to **User Management** → **User Admin** → **Add User**. Screen capture below depicts the user configured during the compliance test. Note that **CT User** is set to **Yes**.

**Application Enablement Services**
Management Console

Welcome: User cust
Last login: Thu Oct 11 12:40:37 2018 from 10.64.10.202
Number of prior failed login attempts: 0
HostName/IP: aes15019/10.64.150.19
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.3.0.1.7-0
Server Date and Time: Thu Oct 11 17:05:39 MDT 2018
HA Status: Not Configured

User Management | User Admin | Add UserHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▼ User Management

▶ Service Admin

▼ User Admin

▪ Add User

▪ Change User Password

▪ List All Users

▪ Modify Default Users

▪ Search Users

Add User

Fields marked with * can not be empty.

* User Id

* Common Name

* Surname

* User Password

* Confirm Password

Admin Note

Avaya Role

Business Category

Car License

CM Home


Css Home

CT User

Department Number

Display Name

Navigate to **Security** → **Security Database** → **CTI Users** → **List All Users**, and edit the user added above; check box for **Unrestricted Access**.

**Application Enablement Services**
Management Console

Welcome: User cust
Last login: Thu Oct 11 12:40:37 2018 from 10.64.10.202
Number of prior failed login attempts: 0
HostName/IP: aes15019/10.64.150.19
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.3.0.1.7-0
Server Date and Time: Thu Oct 11 17:06:21 MDT 2018
HA Status: Not Configured

Security | Security Database | CTI Users | List All UsersHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▼ Security

▶ Account Management

▶ Audit

▶ Certificate Management

▶ Enterprise Directory

▶ Host AA

▶ PAM

▼ Security Database

Edit CTI User

User Profile:

User ID

Common Name

Worktop Name

Unrestricted Access ☒

Call and Device Control:

Call Origination/Termination and Device Status

Call and Device Monitoring:

Device Monitoring

Calls On A Device Monitoring

Call Monitoring ☐

Routing Control:

Allow Routing on Listed Devices

Apply Changes Cancel Changes

6.2. Obtain Tlink

Obtain the Tlink that will be used by FIL Admin server to connect to AES. Navigate to **Security** → **Security Database** → **Tlinks** and note the Tlink.



Application Enablement Services Management Console

Welcome: User cust
Last login: Thu Oct 11 12:40:37 2018 from 10.64.10.202
Number of prior failed login attempts: 0
HostName/IP: aes15019/10.64.150.19
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.3.0.1.7-0
Server Date and Time: Thu Oct 11 17:07:05 MDT 2018
HA Status: Not Configured

Security | Security Database | Tlinks

[Home](#) | [Help](#) | [Logout](#)

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▼ Security

Tlinks

Tlink Name

- ☒ AVAYA#CM15014#CSTA#AES15019
- ☐ AVAYA#CM15014#CSTA-S#AES15019

[Delete Tlink](#)

7. Configure Avaya Aura® Experience Portal

Experience Portal is configured via the Experience Portal Manager (EPM) web interface, to access the web interface, enter `http:// "ip-address"/` as the URL in a web browser, where “ip-address” is the IP address of Experience Portal. Log in using the appropriate credentials.



Note: Some of the screens in this section are shown after the Experience Portal had been configured. Don't forget to save the screen parameters as Experience Portal is configured.

7.1. Configure FIL Application

In the **Applications** page, add an Experience Portal application to handle incoming calls. This application will perform EWT calculations and provide the caller the option to either continue waiting in the agent queue or to request a call back, or route the call back to Communication Manager. Configure the application as shown below.

Note that the **Called Number** configured is the extension configured in Vector 21 using the V2 variable as configured in **Section 5.4**.

The screenshot shows the Avaya Aura Experience Portal 7.2.1 (ExperiencePortal) configuration interface. The top navigation bar includes the Avaya logo, a welcome message for 'epadn', and a timestamp 'Last logged in today at 2:53:37 PM'. The left sidebar contains a tree view with categories: User Management, Real-time Monitoring, System Maintenance, System Management, System Configuration, Security, Reports, and Multi-Media Configuration. The main content area is titled 'Use this page to change the configuration of an application.' and displays the configuration for the 'FIL_Test' application. The configuration fields include: Name (FIL_Test), Enable (Yes/No), Type (VoiceXML), Reserved SIP Calls (None/Minimum/Maximum), Requested (empty), URI (Single/Fail Over/Load Balance), VoiceXML URL (http://10.64.110.155:7080/SF_FIL_IVR_V2_0/Start), Mutual Certificate Authentication (Yes/No), Basic Authentication (Yes/No), Speech Servers (ASR: LumenVox, Languages: en-AU, Selected Languages: en-US), TTS (No TTS), and Application Launch (Inbound/Inbound Default/Outbound, Number/Number Range/URI, Called Number: 51111). Buttons for 'Verify', 'Add', and 'Remove' are present.

AVAYA

Welcome, epadn
Last logged in today at 2:53:37 PM

Avaya Aura® Experience Portal 7.2.1 (ExperiencePortal)

Expand All | Collapse All

- ▼ User Management
 - Roles
 - Users
 - Login Options
- ▼ Real-time Monitoring
 - System Monitor
 - Active Calls
 - Port Distribution
- ▼ System Maintenance
 - Audit Log Viewer
 - Trace Viewer
 - Log Viewer
 - Alarm Manager
- ▼ System Management
 - EPM Manager
 - MPP Manager
 - Software Upgrade
 - System Backup
- ▼ System Configuration
 - Applications
 - EPM Servers
 - MPP Servers
 - SNMP
 - Speech Servers
 - VoIP Connections
 - Zones
- ▼ Security
 - Certificates
 - Licensing
- ▼ Reports
 - Standard
 - Custom
 - Scheduled
- ▼ Multi-Media Configuration
 - Email
 - HTML
 - SMS

Use this page to change the configuration of an application.

Name: FIL_Test

Enable: ☒ Yes ☐ No

Type: VoiceXML

Reserved SIP Calls: ☒ None ☐ Minimum ☐ Maximum

Requested:

URI

☒ Single ☐ Fail Over ☐ Load Balance

VoiceXML URL: http://10.64.110.155:7080/SF_FIL_IVR_V2_0/Start **Verify**

Mutual Certificate Authentication: ☐ Yes ☒ No

Basic Authentication: ☐ Yes ☒ No

Speech Servers

ASR: LumenVox

Languages: en-AU

Selected Languages: en-US

TTS: No TTS

Application Launch

☒ Inbound ☐ Inbound Default ☐ Outbound

☒ Number ☐ Number Range ☐ URI

Called Number: 51111 **Add**

51111 **Remove**

At the bottom of the page, expand **Advanced Parameters** and configured the fields as highlighted below.

AVAYA Welcome, epad
Last logged in today at 2:53:37 PM

Avaya Aura® Experience Portal 7.2.1 (ExperiencePortal) Home ? Help Log

Expand All | Collapse All

- ▼ **User Management**
 - Roles
 - Users
 - Login Options
- ▼ **Real-time Monitoring**
 - System Monitor
 - Active Calls
 - Port Distribution
- ▼ **System Maintenance**
 - Audit Log Viewer
 - Trace Viewer
 - Log Viewer
 - Alarm Manager
- ▼ **System Management**
 - EPM Manager
 - MPP Manager
 - Software Upgrade
 - System Backup
- ▼ **System Configuration**
 - Applications
 - EPM Servers
 - MPP Servers
 - SNMP
 - Speech Servers
 - VoIP Connections
 - Zones
- ▼ **Security**
 - Certificates
 - Licensing
- ▼ **Reports**
 - Standard
 - Custom
 - Scheduled
- ▼ **Multi-Media Configuration**
 - Email
 - HTML
 - SMS

☒ Inbound ☐ Inbound Default ☐ Outbound

☒ Number ☐ Number Range ☐ URI

Called Number: **Add**

Remove

Speech Parameters ▶

Reporting Parameters ▶

Advanced Parameters ▼

Support Remote DTMF Processing: ☐ Yes ☒ No

DTMF Type Ahead Enabled: ☒ Yes ☐ No

Converse-On: ☐ Yes ☒ No

Network Media Service: ☐ Yes ☒ No

Early Media: ☐ Yes ☒ No

Sync FROM and PAI Headers: ☐ Yes ☒ No

Dialog URL Pattern:

VoiceXML Event Handler:

CCXML Event Handler:

Generate UCID: ☒ Yes ☐ No

Operation Mode:

Transport UCID in Shared Mode: ☒ Yes ☐ No

Maximum UUI Length:

Fax Detection Enabled: ☐ Yes ☒ No

Fax Phone Number:

Video Enabled: ☐ Yes ☒ No

Video Screen Format:

Video Minimum Picture Interval:

7.2. Configure Outcall Authentication

Configure the Outcall User Name and Password that will be sent by FIL Outbound module to initiate a call back. Click on **EPM Servers** in the left pane, in the resulting page, click on **EPM Settings** (not shown) to display the page below. Under the **Outcall** section, configure the **User Name** and **Password** used by FIL when it makes an outcall request to Experience Portal.

AVAYA

Welcome, epadmin
Last logged in today at 10:29:43 AM PDT

Avaya Aura® Experience Portal 7.2.1 (ExperiencePortal)

Expand All Collapse All

User Management

- Roles
- Users
- Login Options

Real-time Monitoring

- System Monitor
- Active Calls
- Port Distribution

System Maintenance

- Audit Log Viewer
- Trace Viewer
- Log Viewer
- Alarm Manager

System Management

- EPM Manager
- MPP Manager
- Software Upgrade
- System Backup

System Configuration

- Applications
- EPM Servers
- MPP Servers
- SNMP
- Speech Servers
- VoIP Connections
- Zones

Security

- Certificates
- Licensing

Reports

- Standard
- Custom
- Scheduled

Multi-Media Configuration

- Email
- HTML
- SMS

You are here: [Home](#) > [System Configuration](#) > [EPM Servers](#) > EPM Settings

EPM Settings

Use this page to configure system parameters that affect the Experience Portal system.

Experience Portal Name:

ExperiencePortal

Number of Application Server Failover Logs:

10

Commands to Retain in Configuration History:

50

Resource Alerting Thresholds (%)

HTML Units:

80

Disk:

High Water

90

Low Water

80

Web Service Authentication

Application Reporting

User Name:

<Default>

Password:

.....

Verify Password:

.....

Outcall

User Name:

admin

Password:

.....

Verify Password:

.....

KJA; Reviewed:
SPOC 11/30/2018

Solution & Interoperability Test Lab Application Notes
©2018 Avaya Inc. All Rights Reserved.

23 of 30
SFFIL-AEP72

8. Configure First In Line™

Swampfox First In Line™ offers many configuration options to support varied call center telephony environments. See www.swampfoxinc.com to view details of the First In Line™ product along with the entire suite of products and solutions available. This document will provide the application configuration information used during the compliance testing.

Call Vectoring setup associated with First In Line configuration information below is available in **Section 5.4**. During the compliance testing, configuration for FIL was performed by Swampfox, Inc engineers.

8.1. Test Queue Setup

Configuration for FIL is performed via a First In Line admin portal, <http://<IP-Address>:8080/fil>, where IP-Address is the IP Address of the server running FIL. After logging on, the user lands at the **Queues** page. During the compliance test, “Test queue” was created as shown below:

The screenshot displays the 'First In Line' admin portal interface. The top navigation bar shows 'My FIL Site > Queues'. A search bar is present with the text 'I want to search Queues for...'. The main content area shows a table titled 'Queues' with '1 total' entry. The table has columns: Name, State, Skill Extension, AES Connection, Time Zone, Schedule, Callback Schedule, and Calendar. The single entry is 'Test queue' with a state of 'OFFERING'. The left sidebar contains a menu with items: Dashboard, Queues, Queue Groups, Offer VDNs, Queue Schedules, Callback Schedules, Calendars, Prompts, Settings, Reports, User Management, and About Dashboard.

	Name ↓	State	Skill Extension	AES Connection	Time Zone	Schedule	Callback Schedule	Calendar
<input type="checkbox"/>	Test queue	OFFERING	22231	FIL Cert AES	US/Mountain	Sample Schedule	Test Callback Schedule	

Rows per page: 10

Clicking on the Queue name takes the user to the Queue Setup page for that queue.

Here the queue **Mode** is set to “OFFER” and VDN 22221 was configured as the **Offer VDN** for this test queue. Skill and Skill Extension number must be provided for queue monitoring purposes, 21 and 22231 as configured in **Section 5.2**.

My FIL Site > Queues > Test queue

Configuration | Schedule Mgmt | Callbacks | Monitoring VDNs | Overrides | Queue Parameters

General

☒ Enabled

Mode
OFFER

Name *
Test queue

Description

Skill *
21

Skill Extension *
22231

Time Zone *
US/Mountain

Queue Group
Test Group

AES Connection
FIL Cert AES

Offer VDNs | 1 total | Manage

22221

BSR Polling VDN

Business Reporting

Saved Call Value *
10.00

Pre-FIL Abandonment Rate *
100.00

Cancel Save

Selecting **Monitoring VDNs** from the list of sections in the Test queue screen above will take the user to the list of monitoring VDNs. All VDNs that may be queued to this skill must be entered into this section for the application to monitor estimated wait times associated with this queue. In this simple test configuration, the only Monitoring VDNs are the No Callback and Callback VDNs.

- No Callback VDN: The VDN transferred to if FIL does not make an offer (various reasons can cause this)
- Callback VDN: The VDN transferred to when a callback offer is made and FIL calls the calling party back and receives a live voice answer.

The Offer, No Callback (Queue VDN), and Callback VDNs are configured on the Offer VDN page available from the First In Line home screen. Following was configured during the compliance test.

First In Line | My FIL Site > Offer VDNs

Search

Offer VDNs | 1 total

	VDN	Queue VDN	Callback VDN	Description	Queue	Language	Announcements
<input type="checkbox"/>	<input type="text" value="VDN"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="Description"/>		<input type="text" value="english"/>	<input type="checkbox"/>
<input type="checkbox"/>	22221	22222	22223	Offer VDN	Test queue	english	4

Rows per page 10

Test Queue and Callback Schedules were also setup for testing. These are required so that the application knows only to make callbacks during time periods when the call center is open.

9. Verification Steps

This section provides the verification steps that may be performed to verify that Experience Portal can run FIL applications.

1. From the EPM web interface, verify that the EPM/MPP server is online and running in the **System Monitor** page shown below.

The screenshot shows the 'System Monitor' page in the Avaya Aura Experience Portal 7.2.1. The page title is 'System Monitor (Sep 28, 2018 8:41:51 AM PDT)'. It includes a navigation sidebar on the left with categories like User Management, Real-time Monitoring, System Maintenance, System Management, System Configuration, and Security. The main content area shows a summary of the local Experience Portal system and any remote systems configured. A table displays the current state of the local system, including call capacity and active calls.

Server Name	Type	Mode	State	Config	Call Capacity	Active Calls	Alarms				
					Current	Licensed	Maximum	In	Out	Today	
EPM / localMPP	EPM/MPP	Online	Running	OK	5	5	10	0	0	0	✓
Summary					5	5	10			0	✓

2. From the EPM web interface, verify that the ports on the MPP server are in-service in the **Port Distribution** page shown below.

The screenshot shows the 'Port Distribution Report' page in the Avaya Aura Experience Portal 7.2.1. The page title is 'Port Distribution Report (Oct 11, 2018 4:13:46 PM PDT)'. It includes a navigation sidebar on the left. The main content area shows information about how telephony resources have been distributed to the MPPs. A table displays the current state of the ports, including port group, protocol, and allocation.

Port	Mode	State	Port Group	Protocol	Current Allocation	Base Allocation
10	Online	In service	ASM	SIP_Trunk	localMPP	

3. Place a call to the inbound VDN configured in **Section 5.4** and verify call back options are played by the FIL Inbound module.
 - a. In order to hear call back options, an estimated wait time (EWT) must be seen for the queue associated with the inbound call. This requires multiple calls queued to agents with no agents available to service them. Some number of those calls must have arrived at different points in time (e.g. 5 min between calls). Alternatively, the EWT may be forced to a value that will cause the callback options to be offered for all calls. This is accomplished by setting (via the FIL portal) the advanced configuration parameter queue.override.ewt to some value greater than the minimum threshold for callback offers.

4. Continuing from above, select a call back option so the FIL Outbound module adds a call back request in the database.
5. Via the Dashboard portion of the First In Line™ admin portal, verify that offer(s) have been made and callback(s) are pending.
6. Verify that the callback is received in the time interval announced and on the number selected during the offer dialog.

10. Conclusion

These Application Notes describe the configuration steps required to integrate the First In Line™ by Swampfox Technologies, Inc with Avaya Aura® Application Enablement Services and Avaya Aura® Experience Portal. All feature and serviceability test cases were completed successfully.

11. Additional References

This section references the Avaya documentation relevant to these Application Notes. The following Avaya product documentation is available at <http://support.avaya.com>.

- [1] Administering Avaya Aura® Communication Manager, Release 7.1.3, Issue 7, May 2018
- [2] Administering and Maintaining Avaya Aura® Application Enablement Services, Release 7.1.3, Issue 5, May 2018
- [3] Administering Avaya Aura® Experience Portal, Release 7.2.1, Issue 1, March 2018

Product Documentation for Swampfox FIL can be obtained directly from Swampfox.

©2018 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.